ROUTING AND TRANSMITTAL SLIP Date 7 Apr '80

TO: (Name, office symbol, room number, building, Agency/Post)	Initials	Date
1. DDA		
2.		
3.		
4.		
5.		

✓	Action		File		Note and Return
	Approval		For Clearance		Per Conversation
	As Requested		For Correction		Prepare Reply
	Circulate		For Your Information		See Me
	Comment		Investigate		Signature
	Coordination		Justify		

REMARKS

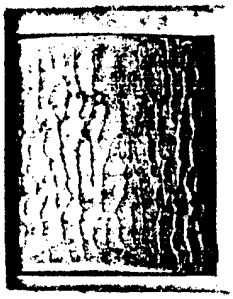
DO NOT use this form as a RECORD of approvals, concurrences, disposals, clearances, and similar actions

FROM: (Name, org. symbol, Agency/Post)	Room No.—Bldg.
D/ES	Phone No.

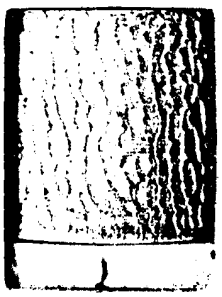
5041-102

OPTIONAL FORM 41 (Rev. 7-76)
Prescribed by GSA
FPMR (41 CFR) 101-11.206

☆ U. S. Government Printing Office: 1979—281-184/8



STAT



L-116
PD-24

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF SCIENCE AND TECHNOLOGY POLICY
WASHINGTON, D.C. 20500

April 2, 1980

MEMORANDUM FOR: The Secretary of State
The Secretary of Treasury
The Secretary of Defense
The Attorney General
The Secretary of Commerce
The Secretary of Transportation
The Secretary of Energy
Director of Central Intelligence ✓
Assistant to the President for National Security Affairs
Administrator, General Services Administration
Director, National Security Agency

ALSO: The Director, Office of Management and Budget
The Assistant to the President for Domestic Affairs
The Manager, National Communications System
Chairman, Federal Communications Commission

FROM: Frank Press

SUBJECT: Telecommunications and Information Vulnerability Surveys

The National Telecommunications and Information Administration of the Department of Commerce was tasked as part of their PD/NSC-24 responsibilities, to conduct in 1979, surveys of five U.S. Government agencies. Their purpose was to attempt to identify unclassified information -- not related to national security -- that might require protection.

I have attached a copy of the survey teams findings because I feel that they are of such a nature as to warrant your individual review.

The substance of these surveys reflects the necessity for positive action. I suggest that you make these findings known throughout your organization and as applicable use them as a basis for initiating personnel awareness and information protection programs.

Attachment

SUMMARY OF FINDINGS OF TELECOMMUNICATIONS AND INFORMATION VULNERABILITY SURVEYS

I. INTRODUCTION

During 1979 the Special Project Office of NTIA completed five telecommunications and information vulnerability surveys in the federal civil sector and had three more in progress. This report summarizes the findings of these surveys. Each survey performed by NTIA for a client agency is terminated with the issuance of a survey report, which documents specific findings and offers NTIA's recommendations for corrective action. Only the findings are discussed below; the organizations from which they were developed are not identified.

II. THE SURVEY SAMPLE

The eight survey projects undertaken by NTIA in 1979 include a broad sample of federal civil governmental activities. Surveys were performed of one agency specializing in socioeconomic matters, one specializing in a transportation area, one scientific center, two law enforcement agencies, a regulatory agency, and an organization controlling an aspect of national financial activities. Each survey involved studies of telecommunications resources in depth and interviews of operations, telecommunications, and management personnel. Several hundred interviews have been accomplished to date among the various agencies surveyed.

III. SURVEY FINDINGS

There is no standardized concept of "information sensitivity" among the agencies and government employees generally are unfamiliar with the term. NTIA survey teams consistently note a strong grasp of fundamentals and the requirements for protecting national security information. Even employees who do not routinely work with classified information are capable of distinguishing between classified and unclassified information. This is so because of the standardized document marking procedures required by E.O. 12065. In the case of unclassified, nonnational security sensitive information, however, the surveys find that distinctions between unclassified information which requires protection and unclassified information which does not are blurred at best and are normally not even considered. In contrast to the strong formal programs of security education administered by most agencies, employees are not at all trained in identifying unclassified information which must be protected. This required distinction is new to most employees and is one which quite obviously was never before necessary. Exceptions to this generalization are found in those agency programs which caveat certain categories of information as being "FOR OFFICIAL USE ONLY," "AGENCY SENSITIVE," or "NOT FOR PUBLIC RELEASE." Another exception is found in applications of the Privacy Act. Our surveys find that such programs do alert employees to requirements for special handling of information subject to Privacy Act protection. In some departments, documents marked with these limitations receive handling equal to that given to classified documents. But in no case do the special handling caveats for unclassified information extend to a requirement for telecommunications protection should the contents be sent via electrical means.

2. There is minimal awareness of the vulnerabilities of agency telecommunicaitons facilities to intercept. Few government employees outside of communications jobs are even marginally familiar with the technical aspects of the communications circuits over which they transact routine business. NTIA survey teams have surprised numerous senior employees and many more junior ones by explaining that long-distance telecommunications often travel over terrestrial microwave or satellites paths. Often, "private circuits" leased by agencies for their own special purposes are presumed to afford privacy from intercept as well. (This view is, of course, worse than false. Private leased circuits are more vulnerable to intercept than are the circuits of the public networks.) Many government employees are unaware that any unsecured communication may be intercepted and exploited regardless of its being in speech, data, facsimile, or teletypewriter formats. An exception to this observation is found in the federal law enforcement area, which is discussed below.

3. The general failure of government employees and managers to appreciate the threat to vulnerable telecommunications is understandable. Much of the information available on suspected threats to government communications derives from intelligence sources and is classified. It is quite possible, however, to educate employees about potential threats without divulging any classified information.

4. Unclassified information is freely communicated over unprotected circuits without regard to sensitivity. It unfortunately follows that, in the absence of an appreciation of threat and vulnerability or official guidance on information protection, sensitive government information flows in large volumes over unprotected circuits. This flow is directly proportional to the quantities of sensitive information processed by agencies and exchanged by them with counterparts located elsewhere.

5. Available telecommunications protection resources are under used or are not used at all. Most federal organizations surveyed by NTIA in 1979 were found to have access to secure teletypewriter service provided by GSA Federal Communications Centers, the Department of State, or Department of Defense installations. Others were noted to have access to secure telephone equipments. In no case was it found that there was any routine use of these resources. The reasons for under utilization include, but are not limited to, the following:

a. Employee unawareness of the resource or its location.
b. Employee uncertainty of his own authority to use the resource.
c. Little or no available information about the secure network capabilities.
d. Terminal instruments inconveniently located for general use (e.g., in the office of senior personnel).
e. No official guidance available on the use of resources to protect sensitive unclassified information.
f. Resources at headquarters but not at subordinate levels.

6. Some stereotyped communications patterns compound the vulnerability problems. NTIA surveys have detected regularly scheduled conference calls which link agencies' top management over private circuits. High level instructions, policies and the status of major programs are thus exposed from the most credible organizational sources of information. Other stereotyped patterns include predictable communications flows in reaction to external events and the use of fixed radio frequencies, callsigns, and jargon, all of which aid an eavesdropper in intercepting and exploiting government communications.

7. A reliance on private lines adds to the vulnerability of sensitive telecommunications. As noted in paragraph 2, above, "private" leased circuits do not provide any privacy in the confidentiality sense. Leased circuits are provided to customers by communications carriers, which make those circuits available only to those customers for their exclusive use. The problems facing the would-be interceptor are drastically reduced by the use of leased circuits as opposed to the use of the public network. This is so because of the predicatability of finding the desired agency's traffic always in the same circuit and the knowledge that all the traffic passing over the leased circuit has been orginated by or has been addressed to the target agency.

8. Communications systems managers are currently unprepared to take on the foregoing problems. The typical communications managers with whom the NTIA survey teams have come into contact are essentially inexperienced with requirements for protecting unclassified communications traffic. Their position descriptions do not assign them any responsibilities in this area. Those managers, who work or have worked with cryptosecurity accounts, ordinarily do not sense any requirement to assist their agency colleagues with the protection of unclassified nonetheless sensitive communications traffic. These experts in telecommunications systems are not educated concerning systems vulnerabilities to intercept or on the adversary threat to their agencies.

9. Federal law enforcement activities present an entirely different perspective to the general problems of threat and vulnerability. In the enforcement area, enforcement agents and the employees who work with them are acutely aware of the sensitive nature of their information, the vulnerabilities of their telecommunications resources, and the real threat to the privacy of their operational communications. Several law enforcement agencies are seeking equipment solutions to the vulnerability problems they perceive. NTIA notes that these approaches are uncoordinated. In at least one case with which NTIA has first hand experience, voice scrambler equipments were procured and shortly abandoned after it was learned that the equipments provided no real protection.

NTIA's observations about the federal law enforcement communications are as follows:

a. Some "hot pursuit" conditions are characterized by communications requirements which include highly perishable information for which protection during that instance alone is not required.* Other enforcement activities such as on-going investigations, long-term surveillance, etc., are characterized by high sensitivity and non-perishability of information. This situation is well known by law enforcement managers.

---

*Note, however, that law enforcement tactics may be revealed to unintended listeners during hot pursuit situations for which protection of supporting telecommunications may not be necessary. The exposure of these tactics may be detrimental to the success of future operations.

b. The use of single-channel, fixed frequency radios to support sensitive, non-perishable information exchange requirements undermines other security/privacy arrangements. NTIA observes that static callsigns, lack of protection equipment, and reliance on inadequate codes constitutes a dangerous liability to the success of law enforcement operations. This liability is magnified by the growing threat to agents' radio communications posed by the monitoring of public service radio bands with inexpensive scanners. This threat is well documented in official reports and in the press.

c. Though not related to national security, much law enforcement information is of significant importance. Lack of communications protection resources and procedures makes this information vulnerable to interception and jeopardizes law enforcement missions in areas which are of obvious national interest (drug traffic, customs enforcement, currency counterfeiting operations, immigration control, and the like).